What is Claimed:

1. A method for maintaining the security of a secured execution environment on a system comprising said secured execution environment and a second execution environment, comprising:

accepting user input from a trusted input device;

determining whether said secured execution environment is in a standard input mode; and

if said secured execution environment is in a standard input mode, transferring at least a first portion of said user input to said second execution environment.

2. The method of claim 1, further comprising:

decrypting said user input.

3. The method of claim 1, further comprising:

if said secured execution environment is in a nexus input mode, determining a specific process running in said secured execution environment to which said user input is directed; and

directing said user input to said specific process.

4. The method of claim 1, further comprising:

determining whether said user input comprises a user NIM indication that said secured execution environment should be in a nexus input mode; and

if said user input comprises said user NIM indication and said secured execution environment is not in said nexus input mode, switching said secured execution environment to said nexus input mode.

5. The method of claim 4, where said user NIM indication comprises a combination of keystrokes on a keyboard.

6. The method of claim 4, where said user NIM indication comprises a programmatic activation of a process running in said secured execution environment.

7. The method of claim 6, where said programmatic activation of a first process running in said secured execution environment comprises selecting a graphical user interface element corresponding to said process.

8. The method of claim 7, where said graphical user interface element is a shadow graphical user interface element displayed using a second process, where said process is running on said second execution environment, and where said shadow graphical user interface element corresponds to a secured graphical user interface element displayed by said first process.

9. The method of claim 1, further comprising:

determining whether said user input comprises a user SIM indication that said secured execution environment should be in said standard input mode; and

if said user input comprises said user SIM indication and said secured execution environment is not in said standard input mode, switching said secured execution environment to said standard input mode.

10. The method of claim 9, where said user SIM indication comprises a combination of keystrokes on a keyboard.

11. The method of claim 9, where said user SIM indication comprises an action which results in a display with no graphical user interface element which corresponds to a process running on said secured execution environment.

12. The method of claim 1, where a if said secured execution environment is in a standard input mode, and a second portion of said user input corresponds to changes to a graphical user interface element displayed by a process running on said secured execution

environment, said changes to said graphical user interface element are performed within said secured execution environment.

13. The method of claim 12, where said changes to a graphical user interface element displayed by a process running on said secured execution environment comprise the movement of a mouse cursor over a graphical user interface element displayed by a process running on said secured execution environment.

14. The method of claim 1, further comprising:

switching said secured execution environment to a nexus input mode if a power management change is detected.

15. A computer-readable medium containing computer executable instructions to maintain the security of a secured execution environment on a system comprising said secured execution environment and a second execution environment, the computer-executable instructions to perform acts comprising:

accepting user input from a trusted input device;

determining whether said secured execution environment is in a standard input mode; and

if said secured execution environment is in a standard input mode, transferring at least a first portion of said user input to said second execution environment.

16. The computer-readable medium of claim 15, wherein the computer-executable instructions are adapted to perform acts further comprising:

decrypting said user input.

17. The computer-readable medium of claim 15, wherein the computer-executable instructions are adapted to perform acts further comprising:

if said secured execution environment is in a nexus input mode, determining a specific process running in said secured execution environment to which said user input is directed; and

directing said user input to said specific process.

18. The computer-readable medium of claim 15, wherein the computer-executable instructions are adapted to perform acts further comprising:

determining whether said user input comprises a user NIM indication that said secured execution environment should be in a nexus input mode; and

if said user input comprises said user NIM indication and said secured execution environment is not in said nexus input mode, switching said secured execution environment to said nexus input mode.

19. The computer-readable medium of claim 18, where said user NIM indication comprises a combination of keystrokes on a keyboard.

20. The computer-readable medium of claim 18, where said user NIM indication comprises a programmatic activation of a process running in said secured execution environment.

21. The computer-readable medium of claim 20, where said programmatic activation of a first process running in said secured execution environment comprises selecting a graphical user interface element corresponding to said process.

22. The computer-readable medium of claim 15, where said graphical user interface element is a shadow graphical user interface element displayed using a second process, where said process is running on said second execution environment, and where said shadow graphical user interface element corresponds to a secured graphical user interface element displayed by said first process.

23. The computer-readable medium of claim 15, wherein the computer-executable instructions are adapted to perform acts further comprising:

determining whether said user input comprises a user SIM indication that said secured execution environment should be in said standard input mode; and

if said user input comprises said user SIM indication and said secured execution environment is not in said standard input mode, switching said secured execution environment to said standard input mode.

24. The computer-readable medium of claim 23, where said user SIM indication comprises a combination of keystrokes on a keyboard.

25. The computer-readable medium of claim 23, where said user SIM indication comprises an action which results in a display with no graphical user interface element which corresponds to a process running on said secured execution environment.

26. The computer-readable medium of claim 15, where a if said secured execution environment is in a standard input mode, and a second portion of said user input corresponds to changes to a graphical user interface element displayed by a process running on said secured execution environment, said changes to said graphical user interface element are performed within said secured execution environment.

27. The computer-readable medium of claim 26, where said changes to a graphical user interface element displayed by a process running on said secured execution environment comprise the movement of a mouse cursor over a graphical user interface element displayed by a process running on said secured execution environment.

28. The computer-readable medium of claim 15, wherein the computer-executable instructions are adapted to perform acts further comprising:

switching said secured execution environment to a nexus input mode if a power management change is detected.

29. A trusted user interface engine for use in a computer system comprising a secured execution environment and a second execution environment, said trusted user interface engine comprising:

an input stack for accepting user input; and

a trusted input manager for determining whether said secured execution environment is in a standard input mode; and for directing at least a first portion of said user input to said second execution environment if said secured execution environment is in a standard input mode.

30. The trusted user interface engine of claim 29, where said trusted input manager, if said secured execution environment is in a nexus input mode, determines a specific process running in said secured execution environment to which said user input is directed; and directs said user input to said specific process.

31. The trusted user interface engine of claim 29, where said trusted input manager determines whether said user input comprises a user NIM indication that said secured execution environment should be in a nexus input mode; and if said user input comprises said user NIM indication and said secured execution environment is not in said nexus input mode, switching said secured execution environment to said nexus input mode.

32. The trusted user interface engine of claim 31, where said user NIM indication comprises a combination of keystrokes on a keyboard.

33. The trusted user interface engine of claim 31, where said user NIM indication comprises a programmatic activation of a process running in said secured execution environment.

34. The trusted user interface engine of claim 33, where said programmatic activation of a first process running in said secured execution environment comprises selecting a graphical user interface element corresponding to said process.

35. The trusted user interface engine of claim 34, where said graphical user interface element is a shadow graphical user interface element displayed using a second process, where said process is running on said second execution environment, and where said

shadow graphical user interface element corresponds to a secured graphical user interface element displayed by said first process.

36. The trusted user interface engine of claim 29, where said trusted input manager determines whether said user input comprises a user SIM indication that said secured execution environment should be in said standard input mode; and if said user input comprises said user SIM indication and said secured execution environment is not in said standard input mode, switches said secured execution environment to said standard input mode.

37. The trusted user interface engine of claim 36, where said user SIM indication comprises a combination of keystrokes on a keyboard.

38. The trusted user interface engine of claim 36, where said user SIM indication comprises an action which results in a display with no graphical user interface element which corresponds to a process running on said secured execution environment.

39. The trusted user interface engine of claim 29, where a if said secured execution environment is in a standard input mode, and a second portion of said user input corresponds to changes to a graphical user interface element displayed by a process running on said secured execution environment, said changes to said graphical user interface element are performed within said secured execution environment.

40. The trusted user interface engine of claim 39, where said changes to a graphical user interface element displayed by a process running on said secured execution environment comprise the movement of a mouse cursor over a graphical user interface element displayed by a process running on said secured execution environment.

41. The trusted user interface engine of claim 29, where said trusted input manager switches said secured execution environment to a nexus input mode if a power management change is detected.

42. A method for maintaining the security of a secured execution environment on a system comprising said secured execution environment and a second execution environment, comprising:

maintaining a current state for said secured execution environment selected from among a group of possible states comprising: a standard input mode state and a nexus input mode state;

directing a flow of user input according to said current state.

43. The method of claim 42, further comprising:

limiting a transfer of said user input to said second execution environment when said current state is said nexus input mode state.

44. A computer-readable medium containing computer executable instructions to maintain the security of a secured execution environment on a system comprising said secured execution environment and a second execution environment, the computer-executable instructions to perform acts comprising:

maintaining a current state for said secured execution environment selected from among a group of possible states comprising: a standard input mode state and a nexus input mode state;

directing a flow of user input according to said current state.

45. The computer-readable medium of claim 44, wherein the computer-executable instructions are adapted to perform acts further comprising:

limiting a transfer of said user input to said second execution environment when said current state is said nexus input mode state.